CLAIMS:

1. A method of communicating between a calling party in a first network and a called party in a second network, the method comprising the steps of:

determining in a first network an address associated with a called party;

determining based on said address if said called party is in a trusted network; and

controlling communication between the called party and a calling party based on if said called party is in a trusted network.

2. A method as claimed in claim 1, wherein the step of determining in the first network comprises determining the address contained in a message for said called party.

3. A method as claimed in claim 2, wherein the step of determining in the first network comprises determining the address contained in the message in packet form.

4. A method as claimed in claim 1, wherein the step of determining if the called party is in a trusted network comprises checking if the address is contained in a database of trusted networks.

5. A method as claimed in claim 4, wherein the step of determining if the called party is in a trusted network comprises checking if the address is contained in said database in said first network.

6. A method as claimed in claim 4, wherein the step of determining if the called party is in a trusted network comprises checking if the address is

contained in the database provided in a call session control function or a security gateway.

7. A method as claimed in claim 4, wherein the step of determining if the called party is in a trusted network checking if the address is contained in said database comprising domain names associated with the trusted networks and IP addresses of trusted networks.

8. A method as claimed in claim 1, wherein said step for determining in the first network the address comprises determining if the address contains a domain name.

9. A method as claimed in claim 8, wherein if a determination is made that the address does not contain the domain name, the step of determining in the first network the address comprises sending a request for the domain name.

10. A method as claimed in claim 9, wherein the step of determining in the first network the address comprises sending said request to a domain name server.

11. A method as claimed in claim 8, wherein if a determination is made that the address does not contain the domain name, the step of determing in the first network the address comprises assuming that the called party is in an untrusted network.

12. A method as claimed in claim 1, wherein if the called party is not in a trusted network, the step of controlling comprises discarding at least one message for the called party.

13. A method as claimed in claim 1, wherein if the called party is not in a trusted network, the step of controlling comprises modifying at least one message for the called party.

14. A method as claimed in claim 14, wherein the step of controlling comprises modifying said at least one message for the called party by removing identity information relating to said calling party.

15. A method as claimed in claim 15, wherein the step of controlling comprises removing said identity information comprising a P-Asserted-Identity header.

16. A method as claimed in claim 1, further comprising:

operating said first network and second network in accordance with Session Initiation Protocol .

17. A method as claimed in claim 1, wherein the step of determining if the called party is in a trusted network comprises determining if a connection from a calling network to a called network is secured.

18. A method as claimed in claim 17, wherein the step of determining if the called party is in a trusted network is carried out in an gateway of the calling network.

19. A method as claimed in claim 18, wherein the step of determining if the called party is in a trusted network comprises determining if a connection between a gateway of a calling network and a gateway of a called network comprises a secure connection.

20. A communications system comprising a first network having a calling party and a second network having a calling party, the first network comprising:

determining means for determining an address associated with said called party;

determining means for determining based on said address if said called party is in a trusted network; and

control means for controlling communication between the called party and a calling party based on if said called party is in a trusted network.

21. A first network having a calling party arranged to call a calling party in a second network, the first network comprising:

determining means for determining an address associated with a called party;

determining means for determining based on said address if said called party is in a trusted network; and

control means for controlling communication between the called party and a calling party based on if said called party is in a trusted network.

22. A method of communicating between a calling party in a first network and a called party in a second network, the method comprising the steps of:

determining in a first network if there is a secure connection with a second network; and

if a determination is made that there is no secure connection with said second network, discarding or modifying a message from a calling party to a called party.

23. A method as claimed in claim 22, wherein said step of determining is carried out in a gateway.

25. A method as claimed in claim 24, wherein the step of determining is carried out in said gateway comprising a security gateway.